

LDAP - user management with replication

Kiening Michael

06.06.2011

1 Introduction

The task is to set up a Lightweight Directory Access Protocol (LDAP) server on our virtual debian machines, and replicate each other course members machines as well as act as provider for replication.

2 Installation of needed software

In order to set up LDAP as user management system, we first have to install all needed software, which would be in our case:

- slapd *OpenLDAP server*
- libnss-ldap *NSS module for using LDAP as a naming service*
- ldap-utils *OpenLDAP utilities*
- nscd *Name Service Cache Daemon*

After we have assured all software is installed correctly, we can start setting up our LDAP. In our system we use aptitude as installation-tool. If the first setup configuraion of slapd does not start after installation, it can be started afterwards using *dpkg-reconfigure slapd*.

3 Setting up LDAP as user management system

In this configuration, a root user and a root domain can be defined, for our purpose 'admin' as user and 'course' as domain. The first step is to manage a root account for our LDAP (slapd), that we can access our structures. For this purpose we stop the ldap-server, by */etc/init.d/slapd stop* and open the slapd configuration file, which can be found in */etc/ldap/slapd.d/cn=config/olcDatabase=0config.ldif*, and add a line for the root password in the rootDN-section:

olcRootPW: SSHA^Mre45tuMw^wrx4XY118/19BJMAqjLG01n

the encrypted key passphrase can be acquired using *slappasswd*, which is automatically installed with slapd. The config-file should then look like this:

```

dn: olcDatabase=0config
objectClass: olcDatabaseConfig
olcDatabase: 0config
olcAccess: 0to * by
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth manage by * break
olcRootDN: cn=admin,cn=config
olcRootPW: {SSHA}Mre45tuMwrrx4XY118/19BJMAqjLG01n

```

Now we can start the ldap server again, using */etc/init.d/slapd start*. The basic structure can now be reached via

```
ldapi discover -D cn=admin,dc=course -h ldapi:///
```

Here we can now start to set up our management system:

- add 2 organizational units:
 - add organizational unit people as child of dc=course:


```
add ou=people,dc=course
objectClass: organizationalUnit
ou: people
```
 - add organizational unit labGroup as child of dc=course


```
add cn=labGroup,ou=group,dc=course
objectClass: posixGroup
cn: labGroup
gidNumber: 1014
```
- add users
 - add user as child of people, and member of labGroup


```
add uid=kiening,ou=people,dc=course
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
shadowLastChange: 1
uid: kiening
cn: kiening
gidNumber: 1014
homeDirectory: /home/kiening
sn: Kiening
uidNumber: 1014
userPassword: SSHAx6EkGLcJCWFu3/O+J0ifwTEh+2VSDUL
```

Now our LDAP should be configured as intended. Finally we have to adjust our *nsswitch.conf*, and enable LDAP as valid authentication method, to be able to

log in to our machines using LDAP accounts.

The `nsswitch.conf` is located in `/etc/nsswitch.conf`

We have to add `ldap` here as authentication method in `passwd`, `group` and `shadow`, which looks like this:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the glibc-doc-reference and info packages installed, try:
# info libc Name Service Switch for information about this file.
passwd: compat ldap
group: compat ldap
shadow: compat ldap
hosts: files dns
networks: files
protocols: db files
services: db files
ethers: db files rpc: db files
netgroup: nis
```

Now we can enable LDAP as method to login to unix in PAM:

pam-auth-update

Our user and group entries should now be listed in

- `getent passwd`
- `getent group`

if we now comment the lines for our user and group in

- `/etc/passwd`
- `/etc/groups`
- `/etc/shadow`
- `/etc/gshadow`

we should still be able to log in to our machines, but now using LDAP-authentication.

4 Replication

To set up a replication between our machines, we'll have to configure each machine as provider and replicand at once.

5 Provider

We configure our LDAP as replication provider using the syncprov-overlay. First we have to load the module *syncprov* in our LDAP-system. For this purpose we have to stop our ldap-server, because you can't make changes in a running configuration.

```
/etc/init.d/slapd stop
```

now we can modify the list of loaded modules in

```
/etc/ldap/slapd.d/cn=config/cn=module{0}.ldif
```

in my case the file then looked like this:

```
dn: cn=module{0}
objectClass: olcModuleList
cn: module{0}
olcModulePath: /usr/lib/ldap
olcModuleLoad: {0}back_hdb
olcModuleLoad: {1}syncprov
structuralObjectClass: olcModuleList
entryUUID: a12c94a8-22cf-1030-859b-99d95067222d
creatorsName: cn=admin,cn=config
createTimestamp: 20110604082311Z
entryCSN: 20110604082311.473951Z#000000#000#000000
modifiersName: cn=admin,cn=config
modifyTimestamp: 20110604082311Z
```

now that the syncprov-module is loaded, we can restart the server:

```
/etc/init.d/slapd start
```

To configure the syncprov-overlay, we have to add some entries in the overlay section. We make it a child of 'olcDatabase={1}hdb,cn=config'.

```
vim /etc/ldap/slapd.d/cn=config/olcDatabase={1}hdb.ldif
```

We have to add the replication specific entries here under the section *dn: olcDatabase=1hdb*.

To load the config we add:

```
olcSyncProvConfig: syncprov
olcSpReloadHint: TRUE
olcServerID: 14
```

Like this our machine provides its data for replication on the server-id 14 which means 192.168.16.14, its ip-address.

6 Replicand

For the replication of other providers, we have to add *olcSyncRepl* lines like for replication of my machine:

```
olcSyncRepl: {0}rid=14 provider=ldap://192.168.16.14 searchbase=dc=course
```

```
type=refreshAndPersist retry="60 +" filter=(!(uid=kiening)(&(cn=kiening)(objectClass=posixGroup)))  
bindmethod=simple binddn=cn=replicant,dc=course credentials=guest
```

or

```
olcSyncRepl: {0}rid=2 provider=ldap://192.168.16.2 searchbase=dc=course type=refreshAndPersist  
retry="60 +" filter=(!(uid=lkajan)(&(cn=lkajan)(objectClass=posixGroup)))  
bindmethod=simple binddn=cn=replicant,dc=course credentials=guest
```

which would be the replication of our course leader, or to be more exact, of his LDAP-configuration.